CLAIMS

1. An Identity Generator device (6) arranged for generating a user's service indicator (USI) for a user to access a number of services offered by a service provider (1; 2; 3) through a network operator where user data (4) for the user are accessible, this user's service indicator being usable between the service provider (SP-1; SP-2; SP-N) domain and the network operator (IDP) domain to unambiguously identify the user at each respective domain, the Identity Generator device **characterized in that** it comprises:

   – means for obtaining a master user's identifier (UID) usable to identify the user at the operator's network;

   – means for obtaining a service identifier (SID), indicative of services to be accessed at the service provider; and

   – means (F) for constructing a user's service indicator (USI) that includes the master user's identifier (UID) and the service identifier (SID).

2. The Identity Generator device of claim 1, wherein the service identifier (SID), indicative of services to be accessed at the service provider, comprises at least one element selected from: a service provider indicator (SPI), and a number of service indicators (S1I; SMI).

3. The Identity Generator device of claim 1, further comprising:

   – means for obtaining at least one element selected from: network operator identifier (OID), auxiliary value (Salt), expiry time, and integrity code; and

- means for including the at least one element into the user's service indicator (USI).

4. The Identity Generator device of claim 1, wherein the master user's identifier (UID) is built up as function (SHA-1) of a real user identity (MSISDN).

5. The Identity Generator device of any preceding claim, further comprising means for carrying out a symmetric cipher of the user's service indicator using a ciphering key (K_E).

6. The Identity Generator device of claim 5, wherein the ciphering key (K_E) is unique for all the applicable service providers (1; 2; 3).

7. The Identity Generator device of claim 5, wherein the ciphering key (K_E) is different per each service provider (1; 2; 3).

8. The Identity Generator device of any preceding claim, further comprising a Decomposer component (7) having means for carrying out a reverse generation (F^{-1}) to obtain a master user's identifier (UID) from a given user's service indicator (USI).

9. A Decomposer component (7) having means for carrying out a reverse generation (F^{-1}) to obtain a master user's identifier (UID) from a given user's service indicator (USI), the Decomposer component (7) arranged for integration in, or co-operation with, at least one entity selected from: the Identity Generator device (6) and other entities at the identity provider domain or at the service provider domain.

10. The Decomposer component of claim 9, wherein the means for carrying out a reverse generation (F^{-1}) includes means for obtaining the service identifier (SID) used to generate the given user's service indicator (USI).

11. The Decomposer component of claim 9, wherein the means for carrying out a reverse generation (F^{-1}) may further include means for obtaining at least one element selected from: network operator identifier (OID), and ciphering key (K_E) used to generate the given user's service indicator (USI).

12. The Decomposer component of claim 9, wherein the means for carrying out a reverse generation (F^{-1}) may further include:

   - means for obtaining applicable expiry time criteria; and

   - means for verifying the validity of a given temporary user's service indicator (T-USI) against said expiry time criteria.

13. The Decomposer component of claim 9, further comprising means for verifying the validity of a given user's service indicator (USI) by making use of the master user's identifier (UID) as a search key towards a user directory system (4).

14. A method for generating a user's service indicator (USI) intended for a user (5) to access a number of services offered by a service provider (1; 2; 3) through a network operator where user data (4) for the user are accessible, this user's service indicator being usable between the service provider (SP-1; SP-2; SP-N) domain and the network operator (IDP) domain to unambiguously identify the user at each respective domain, the method **characterized by** comprising:

   - a step of obtaining a master user's identifier (UID) usable to identify the user (5) at the operator's network;

- a step of obtaining a service identifier (SID), indicative of services to be accessed at the service provider; and

- a step of constructing a user's service indicator that includes the master user's identifier and the service identifier.

15. The method of claim 14, wherein the step of obtaining a service identifier includes a step of obtaining at least one element selected from: a service provider indicator (SPI), and a number of service indicators (S1I; SMI).

16. The method of claim 14, further comprising:

- a step of obtaining at least one element selected from: network operator identifier (OID), auxiliary value (Salt), expiry time, and integrity code; and

- a step of including the at least one element into the user's service indicator (USI).

17. The method of claim 14, wherein the step of obtaining a master user's identifier includes a step of applying a function (SHA-1) to a real user identity (MSISDN).

18. The method of claim 14, further comprising a step of carrying out a symmetric cipher of the user's service indicator using a ciphering key (K_E).

19. The method of claim 18, wherein the ciphering key (K_E) is unique for all the applicable service providers.

20. The method of claim 18, wherein the ciphering key (K_E) is different per each service provider.

21. The method of claim 20, further comprising a step of determining a service provider issuing a communication based on a given user's service indicator.

22. The method of any preceding claim, further comprising a step of carrying out a reverse generation (F^{-1}) to obtain the master user's identifier (UID) from a given user's service indicator (USI).

23. A use of the Identity Generator device (6) of claim 1 integrated in, or in close co-operation with, an entity of an identity provider (IDP) network.

24. The use of claim 23, wherein the identity provider (IDP) network is an operator's network where the user data are accessible.

25. The use of claim 24, wherein the entity is a Central Provisioning Entity responsible for provisioning tasks in the operator's network.

26. The use of claim 24, wherein the entity is a User Directory System (4) storing user data.

27. The use of claim 24, wherein the entity is a Border Gateway placed at the border of the operator domain.

28. The use of claim 27, wherein the Border Gateway is an entity selected from: an HTTP Proxy, a WAP Gateway, and a Messaging Gateway.

29. A use of the Decomposer component of claim 9, wherein one of said other entities may be a Border Gateway selected from: an HTTP Proxy, a WAP Gateway, and a Messaging Gateway.